CIS3362 8/25/2025

0) Hack UCF Announcement
1) Substitution Cipher
2) Cryptool

→ Chapter 1 of Code Book by Simon Singh

Plain	Cipher
A →	E
B →	H
C →	K
etc.	

each of the 26 letters has to appear exactly once

Key issue w/ Shift, Affine: small keyspace

If we're willing to make our key more difficult to remember, maybe we'll get better security!

↳ key space = $\frac{26}{A} \times \frac{25}{B} \times \frac{24}{C} \times \ldots \frac{\times 1}{Z} = 26!$

26 factorial $\approx \geq 10^{18}$.

Technique to break a substitution cipher has been around at least since the 900s!
In PRINT, "Al Kindi"

NOT EVERY KEY IS EQUALLY LIKELY!
DIFFERENT LETTERS HAVE DIFFERENT FREQUENCIES IN LANGUAGE
⟹ letter frequencies are unchanged via substitution!

E appears ~ 12.7% time
Z = ~ 0.1% time

Count up letter frequencies it's likely case that more frequent ciphertext letters map to the common letters!

VOWEL/CONSONANT STRUCTURE

REPEATED DIGRAMS/TRIGRAMS/n-GRAMS
↓ ↓
2 3

CRYPTANALYSIS - USE OF CLUES TO REDUCE THE SEARCH FOR POSSIBLE KEY!

Queen Mary of Scots

In time of Queen Elizabeth I. (~1500s)
↳ She imprisoned Mary.
Mary's loyalists wanted to break her out + revolt install her as queen.

More frequent letters had >1 substitution
NULL characters
BACKSPACE CHAR
20 SYMBOLS for common codewords.
} ~ 50 symbols

↳ Barrels of beer they sents messages in outer lines.
↳ hiding fact there was a message.

Sir Francis Walsingham - Elizabeth's Cryptographer.